DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
9301 CHAPEK ROAD,
FORT BELVOIR, VA 22060-5527

REPLY TO
ATTENTION OF

*CPM 380-24
Expires: 24 July 2008

AMCIO-P

24 July 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Memorandum - Common Access Card (CAC)/Public Key Infrastructure (PKI) Guidance for the Use of Digital Signature and Encryption

1. **References:**

a. Department of Defense Instruction (DoDI) 8520.2, ASD (NII), 1 April 04, subject: PKI and Public Key (PK)-Enabling.

b. Memorandum, NETCOM, NETC-EST-A, 2 Sep 03, subject: Army PKI Usage Guidance for Encryption and Digital Signing of E-mail Messages.

c. Memorandum, NETCOM, NETC-EST-A, 3 Jul 03, subject: CAC/PKI Implementation.

2. In anticipation of the release of DoDI 8520.2 (1a, above), the Department of the Army eliminated the mandate requiring digital signature for all e-mail exchanged within the DoD and has issued revised PKI Usage Guidance (1b, above). The revised policy supersedes the Joint CAC/PKI Memorandum (1c, above), as well as all previous DoD policy mandating the wholesale use of digital signatures. In accordance with 1a and 1b, above, this memorandum provides AMC guidance on the use of CAC to digitally sign and/or encrypt e-mail messages.

3. A digital signature provides signer authentication, message integrity and non-repudiation. E-mail encryption ensures confidentiality of information while it is in transit. Per 1b, above, digital signatures should be used whenever e-mail is considered official business and/or Sensitive Information. In accordance with 1b, above, e-mail also should be encrypted when it is necessary to ensure the confidentiality of information that is sensitive but unclassified; protected by the Privacy Act, or protected under the Health Insurance Portability and Accountability Act (HIPAA). General Officers and Senior Executive Service personnel are not specifically addressed in the new PKI Usage Guidance. Their requirements remain unchanged. Additional instruction for sending, receiving, and retaining digitally signed and/or encrypted e-mail is provided in 1b, above and is found at the NETCOM IA – CAC/PKI website (https://iacacpki.army.mil).

---

*This policy memorandum supersedes AMC Policy Memo 380-24, 30 January 2006.

4. At the discretion of Commanders, Life Cycle Management Commands/Separate Reporting Activities (LCMCs/SRAs), Chief Information Officers (CIO) are encouraged to provide more specific guidance regarding the types of data requiring the use of digital signature and encryption for e-mail. Additional guidance should be provided to AMCIO/G-6 for record.

5. The point of contact for this action is Chief, Information Assurance Program Manager at: amcio-IAPM@hqamc.army.mil, AMCIO-P, DSN 656-8577 or (703) 806-8577, AMCIO-P, DSN 656-8824 or (703) 806-8824.

FOR THE COMMANDER:

TERENCE M. EDWARDS
Chief Information Officer/G-6

DISTRIBUTION:
B
H